UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/312,230	05/14/1999	MIKHAIL J. ATALLAH	P00619-US-0	2301

7590 03/08/2004

Thomas A. Walsh
ICE MILLER
One American Square
Box 82001
Indianapolis, IN 46282-0002

EXAMINER	
SMITHERS, MATTHEW	

ART UNIT	PAPER NUMBER
2137	13

DATE MAILED: 03/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/312,230	ATALLAH ET AL.	
	Examiner	Art Unit	
	Matthew B Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 October 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-12,18-23 and 28-82* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *34* is/are allowed.

6)☒ Claim(s) *1,2,4-12,18-23,28-33 and 35-82* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of the Claims

Claims 3, 13-17, and 24-27 were canceled.

Claims 1, 4, 5, 7-12, 18, 19, 28 and 30 were amended.

Claims 34-82 were added.

Claims 1, 2, 4-12, 18-23 and 28-82 are pending.

Response to Arguments

Applicant's arguments filed October 6, 2003 have been fully considered but they are not persuasive.

Applicant argues Matsumoto does not teach classifying the outsourced computations into one of a number of computation types. Examiner contends Matsumoto does teach classifying the computation according to the targeted result sought by the client (first computer) (see section 4, pages 500-502).

Applicant argues Kawamura does not teach classifying the outsourced computations into one of a number of computation types. Examiner contends Kawamura does teach classifying the computation (see pages 779-780; Construction Based on Yao's Algorithm, Construction Based on Knuth's Algorithm, and Further Reduction of the Client's Multiplications).

Applicant argues Casanova does not teach classifying the outsourced computations into one of a number of computation types. Examiner contends Casanova

does teach classifying the computation (see pages 5-6).

Referring to the argument that claim 35 is allowable the examiner inadvertently typed 33 instead of 32 under the Allowable Subject Matter heading but was consistent in the Office Action Summary and the 102 rejection using Matsumoto. It is clear from Office Action Summary and the 102 rejection using Matsumoto that claim 33 was never considered as being allowable subject matter. Therefore claim 35, will be rejected using the same rationale given for the originally presented combination of claims 28 and 33. The examiner maintains the rejection of the originally presented claims and further rejects the newly added claims listed below.

Information Disclosure Statement

The information disclosure statement filed June 30, 2003 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 50-82 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In each of the above listed claims, the process steps are merely an algorithm in which a computer performs a computation on a set of

arguments and subsequently derives a result. The claims only show non-functional descriptive material and do not provide a practical application of the determined result. As such the claims are rejected as non-statutory subject matter.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-22, 24-31, 33, 35, and 37-49 are rejected under 35 U.S.C. 102(a) as being anticipated by "Speeding Up Secret Computations with Insecure Auxiliary Devices" by Matsumoto et al.

Regarding claim 1-2, 13-14, 18, 20, 24-25, 28-29, 35, and Matsumoto shows a client (the second computer) disguises an argument "x" by applying an algorithm "I" to create "u" which is then sent to the server (the first computer). The server computes a result "v" using the disguised input "u" and sends the result "v" back to the client. The client then obtains the actual answer "y" by applying algorithm "F" to the result "v". (see page 499, Paragraph 3).

Regarding claim 3-12, 15-17, 19, 21-22, 26-27, 30-31 and 33, Matsumoto shows basic protocols where matrices are randomly generated at the client and matrix multiplication, linear equations or graph isomorphisms (where permutation matrix X satisfies AX=XB) are used in the process of obtaining the actual answer from an

outsourced computation. (see page 499, Paragraph 3, page 500, Parargraph 4, 4.1(a), 4.1(b) and page 501, paragraph 4.1(c).)

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-2, 13-14, 18, 20, 24-25, 28-29 and 37-49 are rejected under 35 U.S.C. 102(a) as being anticipated by "Fast Server-Aided Secret Computation Protocols for Modular Exponentiation" by Kawamura et al.

Regarding claims 1-2, 13-14, 18, 20, 24-25, 28-29, and 37-49 Kawamura shows a system where a server performs computations for a client without knowing the client's secret information and the client computing the answer from the result computed by the server. (see page 499, Paragraph 3, page 500, Parargraph 4, 4.1(a), 4.1(b) and page 501, paragraph 4.1(c).)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 13-14, 18, 20, 24-25, 28-29, and 37-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Netsolve: A Network for Solving Computational Science Problems" by Casanova et al and further in view of "On Hiding Information from an Oracle" by Abadi et al.

Regarding claims 1-2, 13-14, 18, 20, 24-25, 28-29, 35, and 37-49 Casanova teaches a client-server application designed to solve computational science problems over a network where the server supplies the computational resources needed to service the user's request (see Abstract, page 2, Introduction to page 6, Programming Interfaces and Figure 1). Casanova fails to specifically teach hiding the argument "x" from the server performing the outsourced computation. Abadi teaches a system where a server (the first computer/player B) computes a value for a client (second computer/player A) in such a way that player B cannot determine player A's input value, returns a result for the hiding value and the client further computes the actual answer from the serve computed result (see Abstract and page 4, paragraph 2. Basic definitions to page 6). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Abadi's hiding information from on oracle with Casanova's netsolve system in order to gain the gain the advantage of resources offered by a computing center without having to reveal confidential data [see Abadi et al; page 2, Introduction, Suppose . . . data.].

Allowable Subject Matter

Claim 34 is allowed.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137